PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-010929
(43)Date of publication of application : 14.01.2000

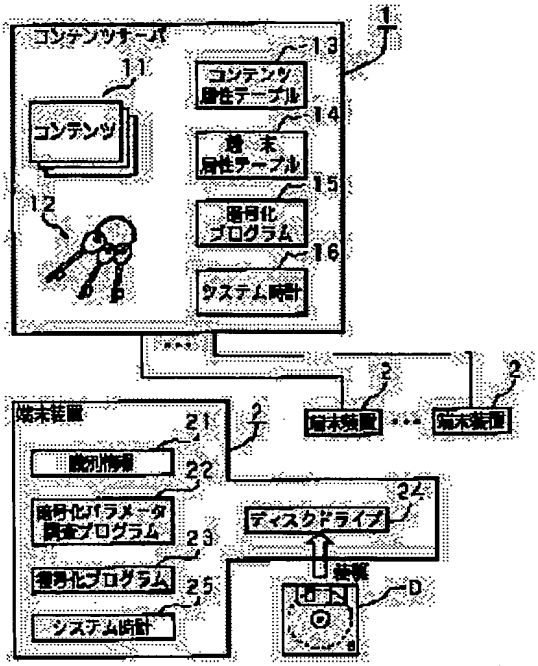
(51)Int.Cl. G06F 15/00
H04L 9/32

(21)Application number : 10-171648
(22)Date of filing : 18.06.1998

(71)Applicant : FUJITSU LTD
(72)Inventor : HIRANO HIDEYUKI

(54) CONTENTS SERVER, TERMINAL DEVICE AND CONTENTS TRANSMISSION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve secrecy for enciphered contents and also to control the enciphered contents stepwise.
SOLUTION: Receiving designation of contents 11 from a terminal device 2, a contents server 1 retrieves a contents attribute table 13 to acquire the secrecy level of the contents 11. The server 1 also retrieves a terminal attribute table 14 for a user of the device 2 related to the designation and acquires the access level of the user. Then, the server 1 compares the access level with the secrecy level of the contents 11 and decides the showing of the secrecy level if the access level is equal to or higher than the secrecy level. The server 1 specifies the identification attribute corresponding to the level and acquires the user ID from the table 14. Then the server 1 enciphers a cipher key 12 of the contents 11 to decode it based on the user ID. The enciphered contents 11 to be decoded by the key 12, the enciphered key 12 and the identification attribute, i.e., the information showing that the identification information used for the encipherment is equal to the user ID are sent to the device 2.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－10929
（Ｐ2000－10929Ａ）
(43)公開日　平成12年１月14日(2000.1.14)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｄ	５Ｂ０８５
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｂ	５Ｋ０１３

審査請求　未請求　請求項の数６　ＯＬ　（全 12 頁）

(21)出願番号　特願平10－171648

(22)出願日　平成10年６月18日(1998.6.18)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　平野　秀幸
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

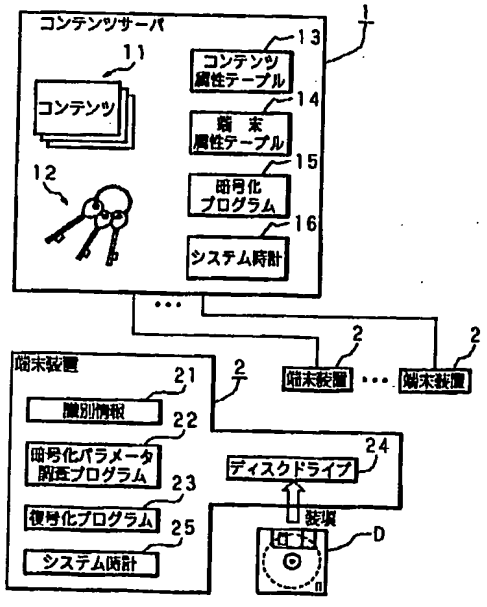
(74)代理人　100078868
弁理士　河野　登夫

Ｆターム(参考)　5B085 AE02 AE06 AE09 AE29
5K013 BA02 FA06 FA08 GA02

(54)【発明の名称】　コンテンツサーバ，端末装置及びコンテンツ送信システム

(57)【要約】
【課題】　暗号化コンテンツの機密性を向上させ、また段階的に調節することを可能にする。
【解決手段】　コンテンツサーバ１は端末装置２からコンテンツ11の指定を受け付けたとき、コンテンツ属性テーブル13を検索して前記コンテンツ11の機密レベルを取得し、またその指定に係る端末装置２のユーザについて、端末属性テーブル14を検索して前記ユーザのアクセスレベルを取得し、これと前記機密レベルとの優位性を比較して、前記アクセスレベルが前記機密レベルと同位か、または前者の方が上位である場合、開示すべしと判定して前記機密レベルと対応付けられた識別属性を特定し、端末属性テーブル14から前記ユーザのユーザＩＤを取得する。コンテンツサーバ１は取得したユーザＩＤを使用して復号化すべく前記コンテンツの暗号鍵12を暗号化し、前記暗号鍵12を使用して復号化すべく暗号化されたコンテンツ及び暗号化された暗号鍵並びに識別属性、即ち暗号化に使用した識別情報がユーザＩＤであるという情報は端末装置２へ送信される。

本発明に係るコンテンツサーバ，端末装置及びコンテンツ送信システムの構成を示すブロック図



1

【特許請求の範囲】

【請求項１】　複数のコンテンツを格納してあり、また複数の端末装置と通信接続し、該端末装置からコンテンツの指定を受け付けたとき、前記コンテンツを暗号化した暗号化コンテンツ及び該暗号化コンテンツを復号化するための暗号鍵を前記端末装置へ送信するコンテンツサーバにおいて、

コンテンツの機密度を表す機密レベルと端末装置側を識別する識別情報の種別を表す識別属性とをコンテンツ毎に対応付けてあるコンテンツ属性テーブルと、

端末装置に設定してあるアクセス権の強さを表すアクセスレベルとその端末装置側を識別する識別情報とを端末装置毎に対応付けてある端末属性テーブルと、

端末装置からコンテンツの指定を受け付けたとき、前記コンテンツ属性テーブルから前記コンテンツの機密レベルを特定し、また前記端末属性テーブルから前記端末装置のアクセスレベルを特定し、該アクセスレベルと前記機密レベルとを比較する手段と、

該手段による比較の結果、両者が同位または前者が上位であるとき、前記コンテンツ属性テーブルから前記コンテンツの識別属性を特定し、また前記端末属性テーブルから前記端末装置について前記識別属性の識別情報を取得し、前記識別情報を使用して復号化すべく前記暗号鍵を暗号化する手段と、

該手段により暗号化された暗号鍵及び前記暗号化コンテンツ並びに前記識別属性を前記端末装置へ送信する手段とを備えることを特徴とするコンテンツサーバ。

【請求項２】　複数のコンテンツを格納してあり、また複数の端末装置と通信接続し、該端末装置からコンテンツの指定を受け付けたとき、前記コンテンツを暗号化した暗号化コンテンツ及び該暗号化コンテンツを復号化するための暗号鍵を前記端末装置へ送信するコンテンツサーバにおいて、

コンテンツの機密度を表す機密レベルと端末装置側を識別する識別情報の種別を表す識別属性とをコンテンツ毎に対応付けてあるコンテンツ属性テーブルと、

端末装置に設定してあるアクセス権の強さを表すアクセスレベルを格納する端末属性テーブルと、

端末装置からコンテンツの指定を受け付けたとき、前記コンテンツ属性テーブルから前記コンテンツの機密レベルを特定し、また前記端末属性テーブルから前記端末装置のアクセスレベルを特定し、該アクセスレベルと前記機密レベルとを比較する手段と、

該手段による比較の結果、両者が同位または前者が上位であるとき、前記コンテンツ属性テーブルから前記コンテンツの識別属性を特定して、前記端末装置へ前記識別属性の識別情報の送信要求を与える手段と、

前記端末装置から識別情報を受信したとき、該識別情報を使用して復号化すべく前記暗号鍵を暗号化する手段と、

2

該手段により暗号化された暗号鍵及び前記暗号化コンテンツ並びに前記識別属性を前記端末装置へ送信する手段とを備えることを特徴とするコンテンツサーバ。

【請求項３】　請求項２に記載のコンテンツサーバと通信接続して、前記コンテンツサーバへコンテンツの指定を与えるための端末装置であって、

前記コンテンツサーバから所定の識別属性の識別情報の送信要求を受け付けたとき、前記識別属性の識別情報を前記コンテンツサーバへ送信する手段と、

前記コンテンツサーバから暗号化された暗号鍵及び暗号化コンテンツ並びに識別属性を受信したとき、前記識別属性の識別情報を使用して前記暗号化された暗号鍵を復号化する手段と、

前記暗号鍵を使用して前記暗号化コンテンツを復号化する手段とを備えることを特徴とする端末装置。

【請求項４】　請求項１に記載のコンテンツサーバ及び該コンテンツサーバと夫々通信接続してコンテンツの指定を与えるための複数の端末装置からなるコンテンツ送信システムであって、

前記端末装置は、

前記コンテンツサーバから暗号化された暗号鍵及び暗号化コンテンツ並びに識別属性を受信したとき、前記識別属性の識別情報を使用して前記暗号化された暗号鍵を復号化する手段と、

前記暗号鍵を使用して前記暗号化コンテンツを復号化する手段とを備えることを特徴とするコンテンツ送信システム。

【請求項５】　請求項２に記載のコンテンツサーバと複数の請求項３に記載の端末装置とを夫々通信接続してあることを特徴とするコンテンツ送信システム。

【請求項６】　複数のコンテンツを格納してあるコンテンツサーバと複数の端末装置とを夫々通信接続してあって、前記コンテンツサーバは前記端末装置からコンテンツの指定を受け付けたとき、前記コンテンツを暗号化した暗号化コンテンツ及び該暗号化コンテンツを復号化するための暗号鍵を前記端末装置へ送信するコンテンツ送信システムにおいて、

前記コンテンツサーバは、

コンテンツの機密度を表す機密レベルをコンテンツ毎に格納するコンテンツ属性テーブルと、

端末装置に設定してあるアクセス権の強さを表すアクセスレベルを端末装置毎に格納する端末属性テーブルと、

端末装置からコンテンツの指定を受け付けたとき、前記コンテンツ属性テーブルから前記コンテンツの機密レベルを特定し、また前記端末属性テーブルから前記端末装置のアクセスレベルを特定し、該アクセスレベルと前記機密レベルとを比較する手段と、

該手段による比較の結果、両者が同位または前者が上位であるとき、前記端末装置へそのシステム時計が示す第１時刻情報の送信要求を与える手段と、

前記端末装置から第１時刻情報を受信したとき、その時点に前記コンテンツサーバのシステム時計が示す第２時刻情報を取得し、該第２時刻情報を使用して復号化すべく前記暗号鍵を暗号化する手段と、

該手段により暗号化された暗号鍵及び前記暗号化コンテンツ並びに第１時刻情報と第２時刻情報との差分情報を前記端末装置へ送信する手段とを有し、

前記端末装置は、

前記コンテンツサーバから第１時刻情報の送信要求を受け付けたとき、前記端末装置のシステム時計が示す第１時刻情報を取得し、該第１時刻情報を記憶するとともに前記コンテンツサーバへ送信する手段と、

前記コンテンツサーバから暗号化された暗号鍵及び暗号化コンテンツ並びに差分情報を受信したとき、記憶した第１時刻情報及び前記差分情報に基づき第２時刻情報を求め、該第２時刻情報を使用して前記暗号化された暗号鍵を復号化する手段と、

前記暗号鍵を使用して前記暗号化コンテンツを復号化する手段とを有することを特徴とするコンテンツ送信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、端末装置からコンテンツの指定を受け付けたとき、前記コンテンツを暗号化した暗号化コンテンツ及び該暗号化コンテンツを復号化するための暗号鍵を送信するコンテンツ送信システム，そのコンテンツサーバ及び端末装置に関する。

【０００２】

【従来の技術】電子化された有料情報、即ちコンテンツを通信ネットワークを介して提供するコンテンツ提供サービスがある。このようなサービスを実施するための最も単純なシステムは、複数のコンテンツを管理するコンテンツサーバ及び該コンテンツサーバと接続してサービスの提供を受ける複数のクライアント（端末装置）により構成される。また一般に、前記サービスにおいて提供されるコンテンツは、そのサービスを行う業者がコンテンツ制作会社から買い取ったものであるか、または前記コンテンツ制作会社からその販売を委託されたものである。前述の如きコンテンツ提供サービスを業として行う上で重要な点は、サービスの提供に応じてその利用者へ料金の支払いを請求する料金請求機構を確実に機能させることである。以下に、前述のシステムにおける料金請求機構の概略を説明する。

【０００３】すなわち、コンテンツサーバはクライアントからのアクセスを受け付けたとき、ユーザ認証処理により前記クライアントを操作するユーザが登録ユーザであることを確認する。その後、商品であるコンテンツを紹介するメニュー情報をクライアント側へ提供し、前記クライアントからのコンテンツ開示要求、即ち注文が与えられるまで待機する。前記コンテンツサーバには暗号

化手段が設けられており、クライアントからの注文を受けると、前記暗号化手段によって前記コンテンツを、所定のパスワードが復号化のための暗号鍵となるように暗号化する。そして、暗号化されたコンテンツ及び前記パスワードを前記クライアントへ送信する。また、前記登録ユーザに対するサービスの料金の支払い請求を発生させる。

【０００４】一方、暗号化されたコンテンツ及びパスワードを受信したクライアントにおいて、前記暗号化されたコンテンツを受信した状態のままでは使用することはできない。前記コンテンツを使用可能にするにはクライアント側において、受信したパスワードを使用して前記コンテンツの暗号化状態を解除する操作を必要とする。このように暗号化状態を解除されたコンテンツを特に、平文コンテンツという。

【０００５】

【発明が解決しようとする課題】ところで、通信ネットワークを介して送信されるコンテンツ及びそれと対応するパスワードは、悪意のユーザに盗聴される虞れがある。すなわち、有料のコンテンツが正規の登録ユーザではないユーザによって不当に入手され、利用されてしまう事態が生じうる。このような事態の発生は、コンテンツ提供サービスを業とする業者の信用低下に係わるだけでなく、前記業者の利益が不当に害される虞れがあるため、その発生を防止すべく送信データの機密性を高める必要がある。

【０００６】また一方で、提供されるコンテンツの提供価格はその内容に応じて設定されているが、設定された提供価格が比較的低いコンテンツについては、その送信に際しての機密度の高さを要求しないという事情がある。例えば、画像データ集，ビジネスレター文例集などは一般に、開発ツールなどのアプリケーションプログラムと比較して安価であり、このようなコンテンツについては、高い機密度は要求されない。しかし、現状では全てのコンテンツについて同様のセキュリティが施されており、前記業者はコンテンツの販売を委託するために、前述の如きコンテンツの提供価格に係わらず一律に同一の料金体系に基づく手数料を支払っている。

【０００７】本発明は、斯かる事情に鑑みてなされた発明であって、暗号化コンテンツと対応する暗号鍵を、複数種類の識別情報のいずれか、またはそれらを組合せて使用して復号化すべく暗号化して送信することにより高い機密性を獲得し、しかも前記組合せに基づき機密性の高さを段階的に調節することを可能になしたコンテンツ送信システム，そのコンテンツサーバ及び端末装置の提供を目的とする。また、時間の経過とともに変化する情報を使用して復号化すべく前記暗号鍵を暗号化して送信することにより機密性を向上を図るコンテンツ送信システムの提供を他の目的とする。

【０００８】

【課題を解決するための手段】第１発明に係るコンテンツサーバは、複数のコンテンツを格納してあり、また複数の端末装置と通信接続し、該端末装置からコンテンツの指定を受け付けたとき、前記コンテンツを暗号化した暗号化コンテンツ及び該暗号化コンテンツを復号化するための暗号鍵を前記端末装置へ送信するコンテンツサーバにおいて、コンテンツの機密度を表す機密レベルと端末装置側を識別する識別情報の種別を表す識別属性とをコンテンツ毎に対応付けてあるコンテンツ属性テーブルと、端末装置に設定してあるアクセス権の強さを表すアクセスレベルとその端末装置側を識別する識別情報とを端末装置毎に対応付けてある端末属性テーブルと、端末装置からコンテンツの指定を受け付けたとき、前記コンテンツ属性テーブルから前記コンテンツの機密レベルを特定し、また前記端末属性テーブルから前記端末装置のアクセスレベルを特定し、該アクセスレベルと前記機密レベルとを比較する手段と、該手段による比較の結果、両者が同位または前者が上位であるとき、前記コンテンツ属性テーブルから前記コンテンツの識別属性を特定し、また前記端末属性テーブルから前記端末装置について前記識別属性の識別情報を取得し、前記識別情報を使用して復号化すべく前記暗号鍵を暗号化する手段と、該手段により暗号化された暗号鍵及び前記暗号化コンテンツ並びに前記識別属性を前記端末装置へ送信する手段とを備えることを特徴とする。

【０００９】第２発明に係るコンテンツサーバは、複数のコンテンツを格納してあり、また複数の端末装置と通信接続し、該端末装置からコンテンツの指定を受け付けたとき、前記コンテンツを暗号化した暗号化コンテンツ及び該暗号化コンテンツを復号化するための暗号鍵を前記端末装置へ送信するコンテンツサーバにおいて、コンテンツの機密度を表す機密レベルと端末装置側を識別する識別情報の種別を表す識別属性とをコンテンツ毎に対応付けてあるコンテンツ属性テーブルと、端末装置に設定してあるアクセス権の強さを表すアクセスレベルを格納する端末属性テーブルと、端末装置からコンテンツの指定を受け付けたとき、前記コンテンツ属性テーブルから前記コンテンツの機密レベルを特定し、また前記端末属性テーブルから前記端末装置のアクセスレベルを特定し、該アクセスレベルと前記機密レベルとを比較する手段と、該手段による比較の結果、両者が同位または前者が上位であるとき、前記コンテンツ属性テーブルから前記コンテンツの識別属性を特定して、前記端末装置へ前記識別属性の識別情報の送信要求を与える手段と、前記端末装置から識別情報を受信したとき、該識別情報を使用して復号化すべく前記暗号鍵を暗号化する手段と、該手段により暗号化された暗号鍵及び前記暗号化コンテンツ並びに前記識別属性を前記端末装置へ送信する手段とを備えることを特徴とする。

【００１０】第３発明に係る端末装置は、請求項２に記載のコンテンツサーバと通信接続して、前記コンテンツサーバへコンテンツの指定を与えるための端末装置であって、前記コンテンツサーバから所定の識別属性の識別情報の送信要求を受け付けたとき、前記識別属性の識別情報を前記コンテンツサーバへ送信する手段と、前記コンテンツサーバから暗号化された暗号鍵及び暗号化コンテンツ並びに識別属性を受信したとき、前記識別属性の識別情報を使用して前記暗号化された暗号鍵を復号化する手段と、前記暗号鍵を使用して前記暗号化コンテンツを復号化する手段とを備えることを特徴とする。

【００１１】第４発明に係るコンテンツ送信システムは、請求項１に記載のコンテンツサーバ及び該コンテンツサーバと夫々通信接続してコンテンツの指定を与えるための複数の端末装置からなるコンテンツ送信システムであって、前記端末装置は、前記コンテンツサーバから暗号化された暗号鍵及び暗号化コンテンツ並びに識別属性を受信したとき、前記識別属性の識別情報を使用して前記暗号化された暗号鍵を復号化する手段と、前記暗号鍵を使用して前記暗号化コンテンツを復号化する手段とを備えることを特徴とする。

【００１２】図５は、第１発明に係るコンテンツサーバを備えるコンテンツ送信システムの概念を説明するための概念図である。前記コンテンツ送信システムは、複数のコンテンツと各コンテンツに所定の暗号鍵とを格納するコンテンツサーバ及び該コンテンツサーバと接続してある複数の端末装置からなる。また前記コンテンツサーバには、コンテンツ毎にその機密レベルと識別属性、具体的にはユーザＩＤ等の端末装置側を識別する識別情報の種別との対応付けを表すコンテンツ属性テーブル及びユーザが使用する端末装置毎にそのアクセスレベルと識別情報、例えば前記ユーザＩＤ等との対応付けを表す端末属性テーブルが格納されている。

【００１３】コンテンツサーバは、端末装置からコンテンツＣｏ の指定を受け付けたとき、前記コンテンツ属性テーブルからコンテンツＣｏ の機密レベルを特定し、また前記端末属性テーブルから前記端末装置のアクセスレベルを特定し、該アクセスレベルと前記機密レベルとを比較する。比較の結果、両者が同位または前者が上位であるとき、コンテンツＣｏ を所定の暗号鍵Ｋｙ を使用して復号化すべく暗号化する。 encＣｏ は、このように暗号化された暗号化コンテンツを表す。また、前記コンテンツサーバは、コンテンツ属性テーブルからコンテンツＣｏの識別属性を取得し、端末属性テーブルから前記識別属性と対応する識別情報を取得してこれを暗号化パラメータＰａ とし、該暗号化パラメータＰａ を使用して復号化すべく暗号鍵Ｋｙ を暗号化する。 encＫｙ は、このように暗号化された暗号化暗号鍵を表す。そして、前記コンテンツサーバは暗号化コンテンツ encＣｏ，暗号化暗号鍵 encＫｙ 及び前記識別属性を前記端末装置へ送信する。

【００１４】暗号化コンテンツ encCo，暗号化暗号鍵 encKy 及び識別属性を受信した端末装置は、まず識別属性に基づき端末装置側において暗号化パラメータPa（即ち、識別情報）を特定し、該暗号化パラメータPaを使用して暗号化暗号鍵 encKy を復号化し、暗号鍵Ky を取り出す。次に、暗号鍵Ky を使用して暗号化コンテンツ encCo を復号化し、コンテンツCo を取り出す。

【００１５】以上の如き手順に基づき指定されたコンテンツCo を送信することによって、コンテンツサーバから端末装置へ送信される全てのデータ、即ち暗号化コンテンツ encCo，暗号化暗号鍵 encKy 及び識別属性が仮に悪意のユーザに盗聴されたとしても、該ユーザにおいて暗号化パラメータPa を特定できないから暗号化暗号鍵 encKy の復号化は叶わず、結果的にコンテンツの不正な利用を防止することができる。またコンテンツ毎に、識別情報の漏洩が生じたとき即時にコンテンツの機密性の喪失とならないように複数の識別属性を設定しておき、一方で端末装置毎の前記識別属性の識別情報を格納しておき、前記識別属性を基づき複数の識別情報を組み合わせて使用すべくなすことにより、機密性の高さを段階的に設定することが可能になる。

【００１６】図６は、第１発明に係るコンテンツサーバを備えるコンテンツ送信システムの動作シーケンスを説明するためのシーケンス図である。前記コンテンツ送信システムは、複数のコンテンツと各コンテンツに所定の暗号鍵とを格納するコンテンツサーバ及び該コンテンツサーバと接続してある複数の端末装置からなる。また前記コンテンツサーバには、コンテンツ毎にその機密レベルと識別属性、具体的にはユーザＩＤ等の端末装置側を識別する識別情報の種別との対応付けを表すコンテンツ属性テーブル及びユーザが使用する端末装置毎にそのアクセスレベルと識別情報との対応付けを表す端末属性テーブルが格納されている。

【００１７】端末装置より発せられる接続要求はコンテンツサーバへ与えられる(A)。コンテンツサーバは接続要求を受けて、コンテンツの概要を掲載したメニューを送信する(B)。端末装置はメニューを受信するとその画面表示を行い(C)、コンテンツの指定を受け付ける。コンテンツを指定する情報はコンテンツサーバへ与えられる(D)。

【００１８】コンテンツサーバはコンテンツの指定を受けてコンテンツ属性テーブルを検索し、該コンテンツに設定された機密レベルを取得する(E)。またその指定に係る端末装置のユーザについて、端末属性テーブルを検索して前記ユーザのアクセスレベルを取得し、これと前記機密レベルとの優位性を比較することにより、開示すべきか否かを判定する(F)。比較の結果、前記アクセスレベルが前記機密レベルより下位である場合、処理を終了する。前記アクセスレベルが前記機密レベルと同位か、または前者の方が上位である場合、開示すべしと判定して前記機密レベルと対応付けられた識別属性を特定し、例えば識別属性としてユーザＩＤが設定されているときは前記ユーザのユーザＩＤを取得する(G)。コンテンツサーバは取得したユーザＩＤを使用して復号化すべく前記暗号鍵を暗号化する(H)。暗号化コンテンツ及び暗号化された暗号鍵並びに識別属性、即ち暗号化に使用した識別情報の種別がユーザＩＤであるという情報は端末装置へ送信される(I)。

【００１９】端末装置は暗号化コンテンツ及び暗号化された暗号鍵並びに識別属性を受信したとき、前記識別属性に基づきユーザＩＤを取得する(J)。そして取得したユーザＩＤを使用して前記暗号化された暗号鍵を復号化し、引き続いて該暗号鍵を使用して前記暗号化コンテンツを復号化する(K)。更に、コンテンツの復号化の結果をコンテンツサーバへ報告する(L)。コンテンツサーバは復号化に成功したことの報告を受けたとき、料金請求を発生させる(M)。

【００２０】このように、前述のコンテンツサーバはコンテンツの指定を受け付けたときに、暗号化コンテンツの復号化に必要な暗号鍵を、端末装置側を識別する識別情報を使用して暗号化し、前記識別情報ではなくその種別、即ち識別属性を端末装置へ通知するため、コンテンツサーバから端末装置へ送信される全てのデータが仮に他のユーザに盗聴されたとしても、該ユーザによる不正な利用を防止することができる。

【００２１】第５発明に係るコンテンツ送信システムは、請求項２に記載のコンテンツサーバと複数の請求項３に記載の端末装置とを夫々通信接続してあることを特徴とする。

【００２２】図７は、第２発明に係るコンテンツサーバ及び複数の第３発明に係る端末装置を備えるコンテンツ送信システムの動作シーケンスを説明するためのシーケンス図である。前記コンテンツ送信システムは、複数のコンテンツと各コンテンツに所定の暗号鍵とを格納するコンテンツサーバ及び該コンテンツサーバと接続してある複数の端末装置からなる。また前記コンテンツサーバには、コンテンツ毎にその機密レベルと識別属性、具体的には後述するメディアＩＤ等の端末装置側を識別する識別情報の種別との対応付けを表すコンテンツ属性テーブル及びユーザが使用する端末装置毎にそのアクセスレベルと識別情報との対応付けを表す端末属性テーブルが格納されている。前記メディアＩＤは端末装置に装填して使用される記録媒体に固有の識別情報であって、ユーザによる書換えが不可能な情報である。

【００２３】端末装置より発せられる接続要求はコンテンツサーバへ与えられる(A)。コンテンツサーバは接続要求を受けて、コンテンツの概要を掲載したメニューを送信する(B)。端末装置はメニューを受信するとその画面表示を行い(C)、コンテンツの指定を受け付ける。コ

ンテンツを指定する情報はコンテンツサーバへ与えられる(D)。

【００２４】コンテンツサーバはコンテンツの指定を受けてコンテンツ属性テーブルを検索し、該コンテンツに設定された機密レベルを取得する(E)。またその指定に係る端末装置のユーザについて、端末属性テーブルを検索して前記ユーザのアクセスレベルを取得し、これと前記機密レベルとの優位性を比較することにより、開示すべきか否かを判定する(F)。比較の結果、前記アクセスレベルが前記機密レベルより下位である場合、処理を終了する。前記アクセスレベルが前記機密レベルと同位か、または前者の方が上位である場合、開示すべしと判定して前記機密レベルと対応付けられた識別属性を特定し、例えば識別属性としてメディアＩＤが設定されているときは前記ユーザが使用する端末装置に装填されているメディアＩＤの提示を前記端末装置へ要求する(G1)。一方、端末装置はメディアＩＤの提示要求を受け付けたとき、暗号化パラメータ調査プログラムを起動させ、前記端末装置のディスクドライブに装填されている記録媒体のメディアＩＤを取得して(G2)、コンテンツサーバへ送信する(G3)。

【００２５】コンテンツサーバはメディアＩＤを受信したとき、該メディアＩＤを使用して復号化すべく前記暗号鍵を暗号化する(H)。暗号化コンテンツ及び暗号化された暗号鍵並びに識別属性、即ち暗号化に使用した識別情報の種別がメディアＩＤであるという情報は端末装置へ送信される(I)。

【００２６】端末装置は暗号化コンテンツ及び暗号化された暗号鍵並びに識別属性を受信したとき、前記識別属性に基づきメディアＩＤを取得する(J)。そして取得したメディアＩＤを使用して前記暗号化された暗号鍵を復号化し、引き続いて該暗号鍵を使用して前記暗号化コンテンツを復号化する(K)。更に、コンテンツの復号化の結果をコンテンツサーバへ報告する(L)。コンテンツサーバは復号化に成功したことの報告を受けたとき、料金請求を発生させる(M)。

【００２７】このように、前述のコンテンツサーバはコンテンツの指定を受け付けたときに、暗号化コンテンツの復号化に必要な暗号鍵を、端末装置側を識別する識別情報を使用して暗号化し、前記識別情報ではなくその種別、即ち識別属性を端末装置へ通知するため、コンテンツサーバから端末装置へ送信される全てのデータが仮に他のユーザに盗聴されたとしても、該ユーザによる不正な利用を防止することができる。またコンテンツ毎に、識別情報の漏洩が生じたとき即時にコンテンツの機密性の喪失とならないように複数の識別属性を設定しておき、一方で端末装置毎の前記識別属性の識別情報を格納しておき、前記識別属性を基づき複数の識別情報を組み合わせて使用すべくなすことにより、機密性の高さを段階的に設定することが可能になる。

【００２８】第６発明に係るコンテンツ送信システムは、複数のコンテンツを格納してあるコンテンツサーバと複数の端末装置とを夫々通信接続してあって、前記コンテンツサーバは前記端末装置からコンテンツの指定を受け付けたとき、前記コンテンツを暗号化した暗号化コンテンツ及び該暗号化コンテンツを復号化するための暗号鍵を前記端末装置へ送信するコンテンツ送信システムにおいて、前記コンテンツサーバは、コンテンツの機密度を表す機密レベルをコンテンツ毎に格納するコンテンツ属性テーブルと、端末装置に設定してあるアクセス権の強さを表すアクセスレベルを端末装置毎に格納する端末属性テーブルと、端末装置からコンテンツの指定を受け付けたとき、前記コンテンツ属性テーブルから前記コンテンツの機密レベルを特定し、また前記端末属性テーブルから前記端末装置のアクセスレベルを特定し、該アクセスレベルと前記機密レベルとを比較する手段と、該手段による比較の結果、両者が同位または前者が上位であるとき、前記端末装置へそのシステム時計が示す第１時刻情報の送信要求を与える手段と、前記端末装置から第１時刻情報を受信したとき、その時点に前記コンテンツサーバのシステム時計が示す第２時刻情報を取得し、該第２時刻情報を使用して復号化すべく前記暗号鍵を暗号化する手段と、該手段により暗号化された暗号鍵及び前記暗号化コンテンツ並びに第１時刻情報と第２時刻情報との差分情報を前記端末装置へ送信する手段とを有し、前記端末装置は、前記コンテンツサーバから第１時刻情報の送信要求を受け付けたとき、前記端末装置のシステム時計が示す第１時刻情報を取得し、該第１時刻情報を記憶するとともに前記コンテンツサーバへ送信する手段と、前記コンテンツサーバから暗号化された暗号鍵及び暗号化コンテンツ並びに差分情報を受信したとき、記憶した第１時刻情報及び前記差分情報に基づき第２時刻情報を求め、該第２時刻情報を使用して前記暗号化された暗号鍵を復号化する手段と、前記暗号鍵を使用して前記暗号化コンテンツを復号化する手段とを有することを特徴とする。

【００２９】前述の如く、暗号化パラメータとして使用される識別情報は通常、一度設定されると頻繁には変更されない。従って、前記識別情報が第三者に知られてしまったときには、その識別情報を使用して復号化すべく暗号化してある暗号鍵が復号化されて、コンテンツが不正に利用される可能性が皆無であるとはいえない。そこで前記コンテンツ送信システムは、時間の経過とともに変化する時刻情報を暗号化パラメータとして使用することにより、コンテンツが不正に利用されないようにするものである。

【００３０】図８は、第６発明に係るコンテンツ送信システムの動作シーケンスを説明するためのシーケンス図である。前記コンテンツ送信システムは、複数のコンテンツと各コンテンツに所定の暗号鍵とを格納するコンテ

ンツサーバ及び該コンテンツサーバと接続してある複数の端末装置からなる。また前記コンテンツサーバには、コンテンツ毎にその機密レベルを表すコンテンツ属性テーブル及びユーザが使用する端末装置毎にそのアクセスレベルを表す端末属性テーブルが格納されている。

【００３１】端末装置より発せられる接続要求はコンテンツサーバへ与えられる(A)。コンテンツサーバは接続要求を受けて、コンテンツの概要を掲載したメニューを送信する(B)。端末装置はメニューを受信するとその画面表示を行い(C)、コンテンツの指定を受け付ける。コンテンツを指定する情報はコンテンツサーバへ与えられる(D)。

【００３２】コンテンツサーバはコンテンツの指定を受けてコンテンツ属性テーブルを検索し、該コンテンツに設定された機密レベルを取得する(E)。またその指定に係る端末装置のユーザについて、端末属性テーブルを検索して前記ユーザのアクセスレベルを取得し、これと前記機密レベルとの優位性を比較することにより、開示すべきか否かを判定する(F)。比較の結果、前記アクセスレベルが前記機密レベルより下位である場合、処理を終了する。前記アクセスレベルが前記機密レベルと同位か、または前者の方が上位である場合、開示すべしと判定して第１時刻情報の提示を端末装置側へ要求する(G1')。一方、端末装置は第１時刻情報の提示要求を受け付けたとき、暗号化パラメータ調査プログラムを起動させ、前記端末装置のシステム時計が示す第１時刻情報を取得して記録し(G2')、またそれをコンテンツサーバへ送信する(G3')。

【００３３】コンテンツサーバは第１時刻情報を受信したとき、その時点の当該コンテンツサーバのシステム時計が示す第２時刻情報を取得し(H1)、第２時刻情報を使用して復号化すべく前記暗号鍵を暗号化する(H2)。暗号化コンテンツ及び暗号化された暗号鍵並びに第１時刻情報と第２時刻情報との差分情報は端末装置へ送信される(I')。

【００３４】端末装置は暗号化コンテンツ及び暗号化された暗号鍵並びに差分情報を受信したとき、記録してある第１時刻情報を読み出す(J')。そして読み出した第１時刻情報及び差分情報から第２時刻情報を特定し(K1)、第２時刻情報を使用して前記暗号化された暗号鍵を復号化し、引き続いて該暗号鍵を使用して前記暗号化コンテンツを復号化する(K2)。更に、コンテンツの復号化の結果をコンテンツサーバへ報告する(L)。コンテンツサーバは復号化に成功したことの報告を受けたとき、料金請求を発生させる(M)。

【００３５】このように、前述のコンテンツ送信システムはコンテンツの指定を受け付けたときに、暗号化コンテンツの復号化に必要な暗号鍵を、コンテンツサーバ側の第２時刻情報を使用して暗号化し、前記第２時刻情報ではなく端末装置側の第１時刻情報と第２時刻情報との差分情報を端末装置へ通知するため、コンテンツサーバから端末装置へ送信される全てのデータが仮に他のユーザに盗聴されたとしても、該ユーザにおいて第２時刻情報を特定して暗号化暗号鍵を復号化することは叶わず、前記ユーザによるコンテンツの不正な利用を防止することができる。

【００３６】

【発明の実施の形態】図１は、本発明に係るコンテンツサーバ，端末装置及びコンテンツ送信システムの構成を示すブロック図である。図において、１は汎用コンピュータを用いてなるコンテンツサーバであり、複数の端末装置2,2,…,2と接続してある。コンテンツサーバ１には、複数のコンテンツ11，各コンテンツに所定の暗号鍵12，コンテンツ毎にその機密レベルと識別属性との対応付けを表すコンテンツ属性テーブル13及びユーザが使用する端末装置毎にそのアクセスレベルと識別情報との対応付けを表す端末属性テーブル14が格納されており、また暗号鍵12を暗号化するための暗号化プログラム15が実装されている。更にまたコンテンツサーバ11はシステム時計16を備える。

【００３７】一方、端末装置２には識別情報21が格納されており、また指定された識別属性の識別情報を暗号化パラメータとして使用すべく取得するための暗号化パラメータ調査プログラム22及び暗号化コンテンツの復号化を行うための復号化プログラム23が実装されている。更にまた端末装置２はディスクドライブ24及びシステム時計25を備える。またディスクドライブ24に装填して使用される記録媒体であるディスクＤには、そのディスクに固有の識別情報、即ちメディアＩＤがユーザによる書換え不可能な領域に書き込まれている。

【００３８】図２はコンテンツサーバ１の処理手順を示すフローチャートである。図６に示すシーケンス図の(E)から(I)と対応付けて説明する。コンテンツサーバ１は端末装置２からコンテンツ11の指定を受け付けたとき、コンテンツ属性テーブル13を検索して前記コンテンツ11の機密レベルを取得する(S2)(E)。またその指定に係る端末装置２のユーザについて、端末属性テーブル14を検索して前記ユーザのアクセスレベルを取得し(S4)、これと前記機密レベルとの優位性を比較することにより、開示すべきか否かを判定する(S6)(F)。比較の結果、前記アクセスレベルが前記機密レベルより下位である場合、処理を終了する。前記アクセスレベルが前記機密レベルと同位か、または前者の方が上位である場合、開示すべしと判定して前記機密レベルと対応付けられた識別属性を特定し、端末属性テーブル14から前記ユーザのユーザＩＤを取得する(S8)(G)。

【００３９】コンテンツサーバ１の暗号化プログラム15は、取得したユーザＩＤを使用して復号化すべく前記コンテンツの暗号鍵12を暗号化する(S10)(H)。そしてコンテンツサーバ１は、暗号化コンテンツ及び暗号化された

暗号鍵並びに識別属性、即ち暗号化に使用した識別情報の種別がユーザＩＤであるという情報を端末装置２へ送信する(S12)(I)。

【００４０】図３はコンテンツサーバ１の他の処理手順を示すフローチャートである。図７に示すシーケンス図の(E) から(I) と対応付けて説明する。コンテンツサーバ１は端末装置２からコンテンツ11の指定を受け付けたとき、コンテンツ属性テーブル13を検索して前記コンテンツ11に設定された機密レベルを取得する(S2)(E) 。

【００４１】またその指定に係る端末装置２のユーザについて、端末属性テーブル14を検索して前記ユーザのアクセスレベルを取得し(S4)、これと前記機密レベルとの優位性を比較することにより、開示すべきか否かを判定する(S6)(F) 。比較の結果、前記アクセスレベルが前記機密レベルより下位である場合、処理を終了する。前記アクセスレベルが前記機密レベルと同位か、または前者の方が上位である場合、開示すべしと判定して前記機密レベルと対応付けられた識別属性を特定し、前記端末装置２のディスクドライブ24に装填されているディスクＤのメディアＩＤの提示を、暗号化パラメータ調査プログラム22へ要求する(S14)(G1) 。

【００４２】コンテンツサーバ１の暗号化プログラム15は、端末装置２からメディアＩＤを受けて(S16) 、該メディアＩＤを使用して復号化すべく前記コンテンツの暗号鍵12を暗号化する(S18)(H)。そしてコンテンツサーバ１は、暗号化コンテンツ及び暗号化された暗号鍵並びに識別属性、即ち暗号化に使用した識別情報はメディアＩＤであるという情報を端末装置へ送信する(S20)(I)。

【００４３】図４はコンテンツサーバ１の他の処理手順を示すフローチャートである。図８に示すシーケンス図の(E) から(I')と対応付けて説明する。コンテンツサーバ１は端末装置２からコンテンツ11の指定を受け付けたとき、コンテンツ属性テーブル13を検索して前記コンテンツ11に設定された機密レベルを取得する(S2)(E) 。

【００４４】またその指定に係る端末装置２のユーザについて、端末属性テーブル14を検索して前記ユーザのアクセスレベルを取得し(S4)、これと前記機密レベルとの優位性を比較することにより、開示すべきか否かを判定する(S6)(F) 。比較の結果、前記アクセスレベルが前記機密レベルより下位である場合、処理を終了する。前記アクセスレベルが前記機密レベルと同位か、または前者の方が上位である場合、開示すべしと判定して前記端末装置２のシステム時計25が示す第１時刻情報の提示を、暗号化パラメータ調査プログラム22へ要求する(S22)(G1')。

【００４５】コンテンツサーバ１の暗号化プログラム15は、端末装置２から第１時刻情報を受けて(S24) 、当該コンテンツサーバ１のシステム時計16が示すその時点の第２時刻情報を取得し(S26)(H1) 、第２時刻情報を使用して暗号化すべく前記コンテンツの暗号鍵12を暗号化する(S28)(H2) 。そしてコンテンツサーバ１は、第１時刻情報と第２時刻情報との差分を算出し(S30) 、暗号化コンテンツ及び暗号化された暗号鍵並びに算出した差分情報は端末装置へ送信される(S32)(I') 。

【００４６】

【発明の効果】以上の如き第１，第２発明のコンテンツサーバ及び第３発明の端末装置並びに第４，第５発明のコンテンツ送信システムによっては、暗号化コンテンツの復号化に必要な暗号鍵を、複数種類の識別情報のいずれか、またはそれらを組合せて使用して復号化すべく暗号化して送信するため、高い機密性を獲得することができ、しかも前記組合せに基づき機密性の高さを段階的に調節することが可能である。従って、コンテンツの委託販売業務において、コンテンツ毎のランク付けに応じて送信するコンテンツの機密性の高さを設定可能にし、その設定に応じて販売を委託した業者へ料金を徴収するような新たなサービスの提供を可能になす。

【００４７】また第６発明のコンテンツ送信システムによっては、コンテンツの指定に係る時刻を表す時刻情報を使用して復号化すべく前記暗号鍵を暗号化して送信することにより機密性を向上を図ることができる。

【図面の簡単な説明】

【図１】本発明に係るコンテンツサーバ，端末装置及びコンテンツ送信システムの構成を示すブロック図である。

【図２】本発明に係るコンテンツサーバの処理手順を示すフローチャートである。

【図３】本発明に係るコンテンツサーバの他の処理手順を示すフローチャートである。

【図４】本発明に係るコンテンツサーバの他の処理手順を示すフローチャートである。

【図５】本発明に係るコンテンツサーバを備えるコンテンツ送信システムの概念を説明するための概念図である。

【図６】本発明に係るコンテンツサーバを備えるコンテンツ送信システムの動作シーケンスを説明するためのシーケンス図である。

【図７】本発明に係るコンテンツサーバ及び端末装置を備えるコンテンツ送信システムの動作シーケンスを説明するためのシーケンス図である。

【図８】本発明に係るコンテンツ送信システムの動作シーケンスを説明するためのシーケンス図である。

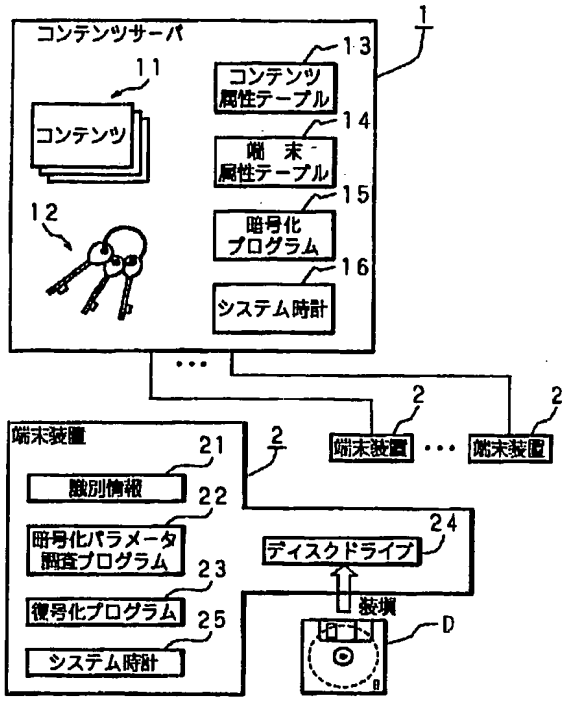
【符号の説明】

1　コンテンツサーバ
11　コンテンツ
12　暗号鍵
13　コンテンツ属性テーブル
14　端末属性テーブル
15　暗号化プログラム
16,25　システム時計

2　端末装置
21　識別情報
22　暗号化パラメータ調査プログラム
＊23　復号化プログラム
24　ディスクドライブ
＊

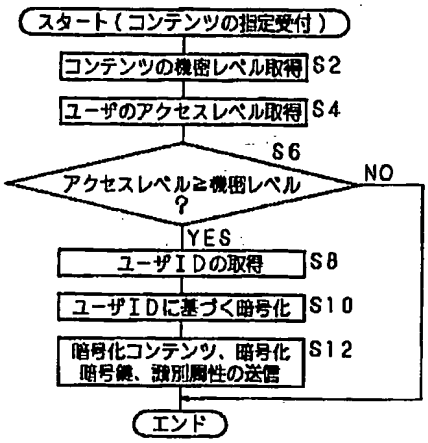
【図１】

本発明に係るコンテンツサーバ，端末装置及びコンテンツ送信システムの構成を示すブロック図



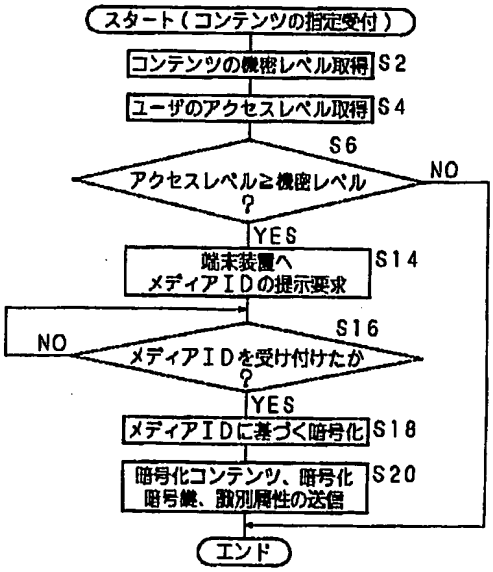
【図２】

本発明に係るコンテンツサーバの処理手順を示すフローチャート



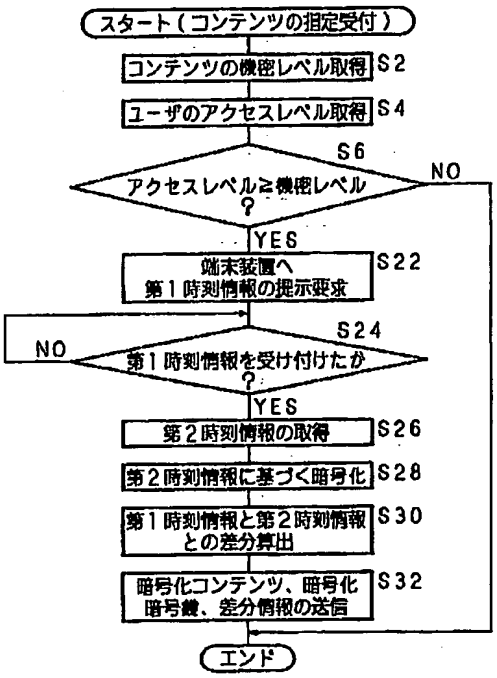
【図３】

本発明に係るコンテンツサーバの他の処理手順を示すフローチャート



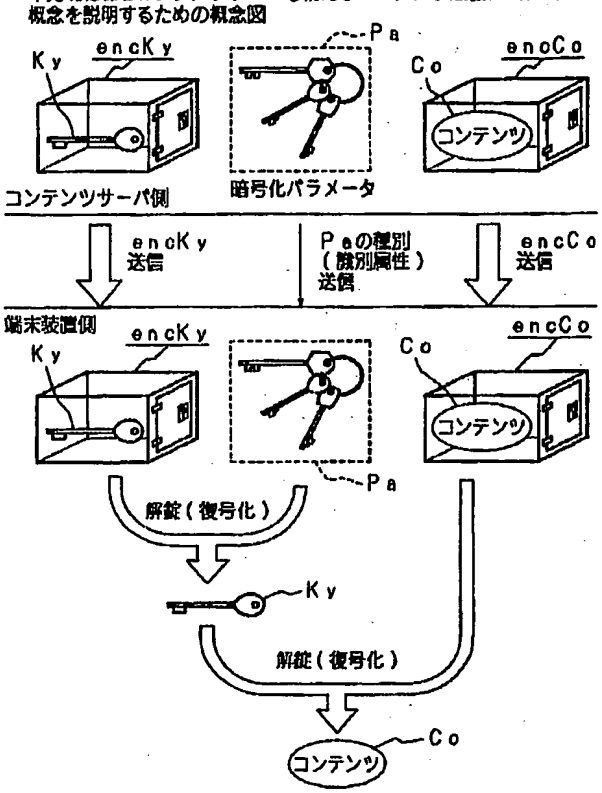
【図４】

本発明に係るコンテンツサーバの他の処理手順を示すフローチャート



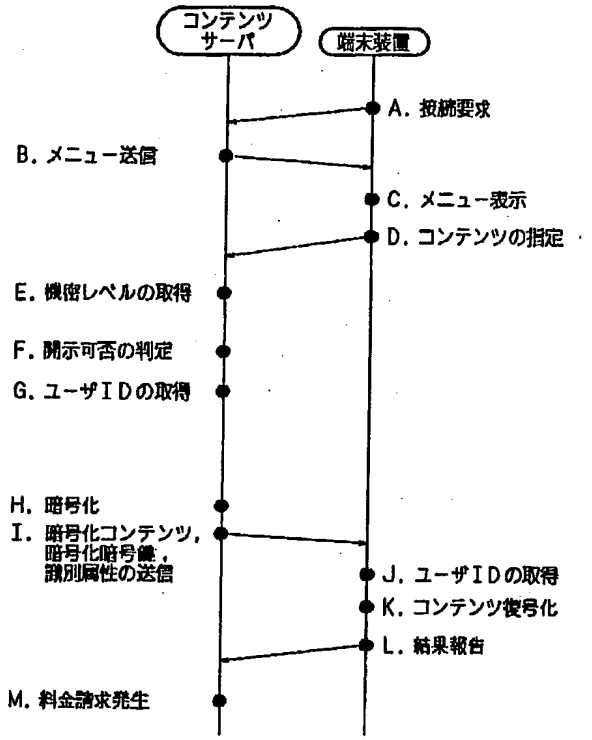
【図５】

本発明に係るコンテンツサーバを備えるコンテンツ送信システムの概念を説明するための概念図



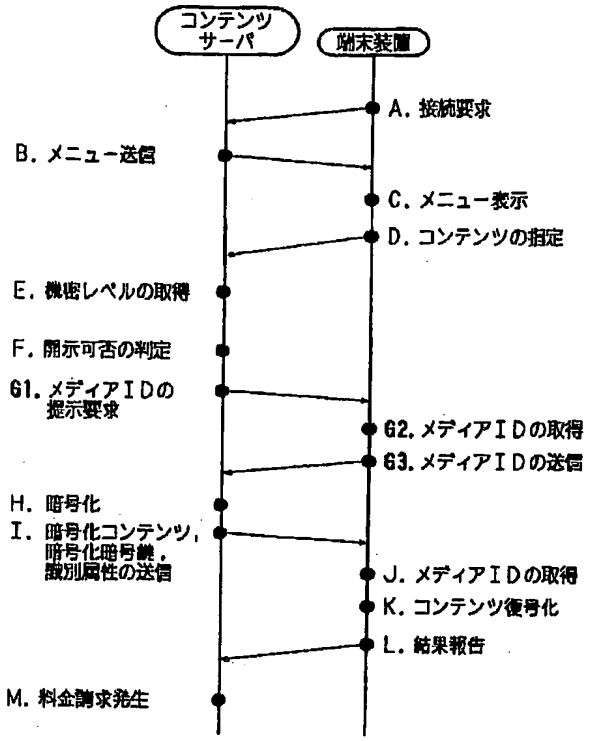
【図６】

本発明に係るコンテンツサーバを備えるコンテンツ送信システムの動作シーケンスを説明するためのシーケンス図



【図７】

本発明に係るコンテンツサーバ及び端末装置を備えるコンテンツ送信システムの動作シーケンスを説明するためのシーケンス図



【図８】

本発明に係るコンテンツ送信システムの動作シーケンスを説明するためのシーケンス図